

FILED

NOV 19 2013

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN RE SEARCH OF
410 TURQUOISE COURT,
MASCOUTAH, ILLINOIS

)
)
)
)
)

Case No. 13-mj-3081-DGW

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF APPLICATION
FOR SEARCH WARRANT**

Your Affiant, Christopher D. Trifiletti, being duly sworn, deposes and states the following:

INTRODUCTION

1. This affidavit is submitted in support of an application for a search warrant, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, to search the residence at **410 Turquoise Court, Mascoutah, St. Clair County, Illinois**, a two-story single family residence with attached garage, displaying the number 410 on the exterior wall between the garage and front door (a photo of which appears in Attachment A), for evidence of federal offenses, including:

Title 18, U.S.C. § 1030 – Fraud and related activity in connection with computers

Whoever . . .

(a)(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (B) information from any department or agency of the United States; or (C) information from any protected computer;

(a)(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States; . . .

(a)(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result

of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if — (A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States;

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section [shall be guilty of a crime.]

2. Your Affiant is a Special Agent with the Federal Bureau of Investigation (FBI), and has been so employed for the past fourteen and a half years. I am currently assigned to the Cyber Squad of the Springfield Field Office and have completed numerous computer intrusion investigations. I have executed search warrants on computers, email accounts, residences, and various types of other digital facilities, conducted review of various types of computer and network logs, interviewed witnesses and subjects related to intrusion investigations, and secured other relevant information using other investigative techniques. I have completed numerous basic and advanced cyber investigative trainings gaining an understanding of the fundamentals of computer hardware, operating systems, computer networks, hacking and malware, information security, and the processing of electronic evidence.

3. The facts set forth in this affidavit are based on your Affiant's personal knowledge, knowledge obtained from other investigators and witnesses, and records and reports. Your Affiant has not included every fact known through the course of the investigation within this affidavit but has included those facts your Affiant believes are sufficient to establish probable cause that the violations set forth above have occurred, and the emails accounts contain evidence, fruits, and/or instrumentalities of violations.

4. As set forth below, there is probable cause to believe that a search of the residence listed above will uncover evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1030, conspiracy to violate 18 U.S.C. § 1030, and/or aid and abet violations of 18 U.S.C. § 1030.

STATEMENT OF FACTS

5. On or about September 3, 2013, United States government personnel working in Maryland discovered that they had lost access to an email account, and a domain¹ originally under the control of a department of the United States government (the “Victim”). Upon attempting to regain access to the email account, Victim personnel realized that the password to the account had been changed and the security challenge question used for password recovery had also been changed. Victim personnel also determined that the password for the account controlling the domain was changed as well. Victim personnel subsequently learned that other website domains controlled by the Victim were targeted by related hacking activity.

6. As part of this investigation, Special Agent Christopher D. Trifiletti swore out an affidavit on September 23, 2013. That affidavit identified Jamie Magers as the likely perpetrator of the malicious activity. Upon a finding of probable cause, United States Magistrate Judge Clifford J. Proud authorized a search warrant for Jamie Magers’s residence, located at

¹ The domains discussed in this affidavit are website domains, of the type that appears in the location box at the top of an Internet browser with the prefix “HTTP” (e.g., <http://www.fbi.gov>). The domains discussed in this affidavit were each maintained on the server of a commercial web-hosting company. Commercial web-hosting companies maintain server computers connected to the Internet for the purpose of hosting website domains. Customers can create an account with the company, and then pay the company to use the web-hosting company’s servers to operate websites on the Internet. Victim personnel registered these domains, rented server space from the web-hosting companies, and then controlled those domains through an account with the web-hosting company (except where, as noted here, unauthorized control of a domain was obtained by a third party).

410 Turquoise Court, Mascoutah, Illinois. *See* No.13-mj-6048-CJP (S.D. Ill.). This affidavit is intended to supplement the information contained in the September 23, 2013, Affidavit (which is incorporated here as Attachment C). This affidavit sets forth additional evidence obtained, in part, from the previous authorized search of the Premises which provides new and further probable cause to believe that there currently exists at the Premises evidence, fruits, and/or instrumentalities of violations of federal criminal law.

7. On September 24, 2013, and at the same time the search warrant was being executed at Magers's residence, FBI agents interviewed Magers at Scott Air Force Base (Magers's place of employment). After being advised that the interview was voluntary, not a requirement of his employment, and that he was free to leave, Magers provided an account of how he had penetrated the Victim's domains and cyber infrastructure. Magers admitted to the malicious activity targeting domains controlled by the Victim agency described in Attachment C. During the September 24 interview, Magers was also advised that a search warrant was simultaneously being executed at his residence. Magers was calm throughout the interview.

8. During his interview, Magers provided an account of what agents would uncover inside his residence. He told agents that they would find a three-gigabyte encrypted volume on his laptop computer and expressly denied that agents would find any devices with full-disk encryption. Magers was unwilling to share his password for the encrypted volume on his laptop.

9. On the morning of September 25, 2013—the morning after his interview and the search of his residence—Magers's fiancé (with whom he lived) informed authorities that he was missing, had taken his firearm, and had left behind a handwritten suicide note. Later that day, authorities discovered Magers in his vehicle with a self-inflicted gunshot wound to the head.

Following his suicide attempt, Magers never regained consciousness. On or about September 28, 2013, Magers was taken off of life support and subsequently died.

10. A portion of the suicide note left by Magers was addressed to “FBI/[Victim]/etc...” and stated: “I know once you go through every thing [sic] you will find things that crossed the line. Nothing I’ve done was meant to hurt anyone. . . . I never planned to leak anything or release anything to the public. . . . If I could go back and undo my wrongs I would. I hope you can see I am a good person at heart, even if I let my curiosity [sic] get the better of me.” Magers’s fiancé also informed investigators that the evening before his suicide, Magers was frantically trying to determine what electronic devices agents had seized. Based on Magers’s statement that investigators will “find things that crossed the line[,]” – a statement made a day after Magers’s calmly admitted to most of the conduct known to investigators – your Affiant believes Magers was involved in additional criminal activity, including unauthorized access, the details of which are not yet known to investigators but could be critical to the Victim.

11. During the September 24 execution of the search warrant at Magers’ residence, several computers and digital media devices were seized. Agents found not only commercial electronic devices, but also many electronic devices and components that appeared to be disassembled, in parts, and hand-built devices. They also found many objects that appeared to be scrap electronics parts. At that stage of the investigation, and due to the voluminous amount of digital media located inside of the residence, a decision was made to seize only the computers and other digital media storage devices deemed likely to contain evidence of Magers’s suspected instructions on the Victim’s domains. Accordingly, some electronic devices and parts were not seized, particularly those that did not appear to be conventional, functioning electronic devices.

However, based on subsequent investigation, agents now believe that some of these devices contain evidence, fruits, and/or instrumentalities of violations of federal law

12. Preliminary forensic analysis of the digital items seized at Magers's residence revealed that Magers did not fully disclose the volume and scope of encrypted media located at his residence. For example, a three-terabyte hard drive that appears to be full-disk encrypted was found attached to one of the computers seized. Preliminary forensic analysis has also failed to locate the three-gigabyte encrypted volume that Magers stated would be on his laptop.

13. Preliminary forensic analysis has also revealed indications of various criminal activity by Magers. This includes:

a) Additional evidence of Magers's compromise of Victim domains was located on Magers laptop computer. For instance, forensic analysis of Magers's devices has located copies of the document containing descriptions of Victim agency infrastructure compromises – previously described in Attachment C, ¶ 9. Several other files associated with the victim's infrastructure were also located on the same computer. Additionally, Google searches specific to Victim domains were also located within information recovered from the Internet browsers on Magers's laptop. Logs of chats between Magers and other associates where Magers specifically detailed his knowledge of and actions against the victim infrastructure were also found on the laptop.

b) In addition to the evidence recovered regarding the compromise of the victim agency, evidence of other crimes has also been found.

i. Magers had accumulated a significant amount of information on one particular individual, to include personal pictures, voicemail recordings, partial credit card information, account passwords, emails, college transcripts, and a significant amount of other

information that would not likely be publicly available. The nature of the information is such that it appears as though Magers was able to access the individual's email account and download all of its contents. It also appears that Magers accessed the voicemail of the individual's boyfriend and downloaded the messages to his computer. Amongst the information collected on this individual were also SQL injection scripts that Magers appears to have used against the website for the university attended by the individual. Investigation is ongoing as to the nature of the relationship between Magers and this individual, and to determine why Magers would have acquired such information.

ii. Similar to the information collected on this individual, it appears that Magers collected information on a particular musical group. Content located on Magers's computer suggests that Magers accessed the email account for the musical group and the individual email accounts of each member of the group. Magers's computer contained copies of records such as pay stubs, contract negotiations, artistic drafts of unreleased album art, copies of passports, personal pictures and videos, and other items related to the musical group and its members that would not be public. Magers is not known to have any relationship with the musical group.

iii. A significant number of username and password databases were also located on Magers's computer. Magers had disclosed the existence of these during his interview, but claimed that he had not obtained any of them through illegal means. He also indicated that he did not use them for unauthorized purposes. However, the preliminary forensic evidence indicates that he was in fact utilizing the information in these databases to access various accounts that did not belong to him.

14. Investigators have also learned that Magers hand-built a number of electronic devices, including devices that were specifically designed to store information and passwords. For instance, investigators believe that there are several so-called “Pass-Pal” devices at Magers’s former residence.

a) Since the search, investigators have examined a website hosted on a domain, OB-Security.info, operated by Magers prior to his death.² Magers hosted a blog at OB-Security.info devoted to the topics of computer hacking, password cracking and related activities. Included on the blog is a posting, dated March 3, 2013, that describes the development of a small, hand-built USB password-storage device he named “Pass-Pal” and describes as a “hardware password and token storage device.” Magers describes the device as an easy way to hold up to twenty complex, unique passwords, and goes on to extol the virtues of this device, stating that it “can hold multiple passwords or tokens, is easy to use and configure, and secure against being compromised if it were lost or stolen.” He also describes the device as mostly complete, except for a case.

b) Investigators also located a YouTube video linked to one of Magers’s identified email accounts, dated June 7, 2013, demonstrating the use of a fully functional “Pass-Pal” device. In the YouTube video, Magers is depicted using the device to log into one of his known email accounts.

² The IP address associated with that domain has been identified as a source of a substantial volume of traffic to many of the Victim domains discussed in Attachment C. During the September 24 interview, Magers also admitted that he used the domain OB-Security.info for some of his activity directed towards the Victim’s domains. The server hosting that website domain OB-Security.info is the subject of a Search Warrant issued in the District of Maryland, No. 13-2225-TJS.

c) At the time of the search of Magers's residence at **410 Turquoise Court, Mascoutah, Illinois**, investigators saw several of these Pass-Pal devices in various stages of completion, but did not seize them because they did not realize the devices were functional. Based on the information set forth above, your Affiant now believes that there is probable cause to believe that at least some of these Pass-Pal devices were functional and that Magers was using the devices to store passwords to his own accounts and encrypted files.

15. Investigators found other references to devices on Magers's blog at OB-Security.info that could be used to circumvent electronic security measures or store sensitive data. For instance, in a post dated January 26, 2013, Magers discussed a "data ex-filtrator" – a device he stated can "transfer data off a secured PC without so much as raising an eyebrow." The hand-built, customized storage device can deceive a computer into thinking that the device is simply a keyboard, and can therefore circumvent security measures in place designed to prevent the unauthorized transfer of data. In his January 2013 blog post, Magers states that he has used the device, and that, "[i]n short order I was copying files from my desktop to the [device] all without the PC ever seeing anything but a USB keyboard." As part of his employment at Scott Air Force Base, Magers had regular access to sensitive and classified materials.

16. Investigators have examined the photographs taken during the September 24, 2013, search of Magers's residence at **410 Turquoise Court, Mascoutah, Illinois**. In one of those photographs is a hand-built device that appears to be the "data ex-filtrator" circumvention device described in the paragraph above.³ Common sense dictates that a person does not need a "data

³ The device in the search warrant photograph is comprised of a small circuit board, known as a "Teensy 2.0" attached to a USB male plug. Mounted to the circuit board is a Micro SD adapter which is another small circuit board that accepts a micro SD storage card. Each of these circuit boards was connected using several wires to a white "breadboard," which is a base used for creating prototype electronic devices.

ex-filtrator” to transfer data off of his own computer – rather, such a device is useful only in extracting data that the user is *not* authorized to copy or retain. The device described by Magers is also a storage device – it contains a micro SD storage card. Even as recently as last week, investigators have been unable to decrypt the data found on Magers’s hard-drive. Any passwords found on those sought devices could be used to decipher that information. Accordingly, your Affiant submits there is probable cause to believe that it is both an instrumentality of a violation of federal law and that it contains evidence and fruits of such a violation. Similarly, due to Magers’s usage of data encryption and password protection equipment and techniques, investigators have probable cause to believe the data and information stored on the other computer devices possessed by Magers may be able to assist in decrypting the information seized in the September 24, 2013 search warrant to better determine the full extent of damage to the Victim and the presence of any other victim(s).

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

18. As described above and in Attachment B, this application seeks permission to search for records that might be found at the residence at **410 Turquoise Court, Mascoutah, Illinois** (“PREMISES”), in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

19. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a

person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a

paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be

sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f) I know that when an individual uses a computer to obtain unauthorized access to a victim computer, domain, or account over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

21. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

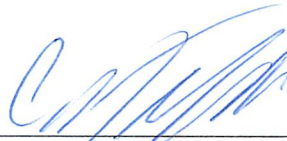
b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

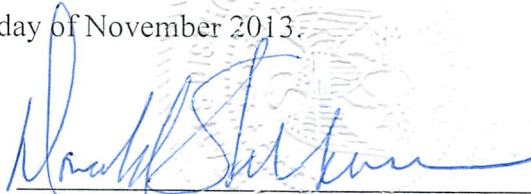
CONCLUSION

23. Based upon the information contained in this affidavit, your Affiant submits that probable cause exists to believe that the residence at **410 Turquoise Court, Mascoutah, Illinois**, contains the evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1030, conspiracy to violate 18 U.S.C. § 1030, and/or aid and abet violations of 18 U.S.C. § 1030.



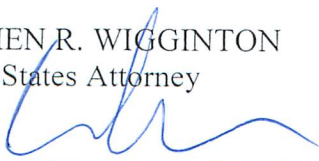
Christopher D. Trifiletti
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this _____ day of November 2013.



DONALD G. WILKERSON
United States Magistrate Judge

STEPHEN R. WIGGINTON
United States Attorney



WILLIAM E. COONAN
Assistant United States Attorney

the Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

Accordingly, the Court finds that the Government has established its burden of proof.

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

The Court's decision in *United States v. [REDACTED]*, 2013 WL 1111111 (S.D. Cal. 2013).

